Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/050360

International filing date: 28 January 2005 (28.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: DE
Number: 10 2004 004 606.9
Filing date: 29 January 2004 (29.01.2004)

Date of receipt at the International Bureau: 19 April 2005 (19.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/EP2005 / 050360

BUNDESREPUBLIK DEUTSCHLAND

EP05/50360
22 03 2005

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	10 2004 004 606.9
Anmeldetag:	29. Januar 2004
Anmelder/Inhaber:	Siemens Aktiengesellschaft, 80333 München/DE
Bezeichnung:	Schaltungsanordnung und Verfahren zur Kommunikationssicherheit innerhalb von Kommunikationsnetzen
IPC:	H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 17. März 2005
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Schmidt C.

Beschreibung

Schaltungsanordnung und Verfahren zur Kommunikationssicherheit innerhalb von Kommunikationsnetzen

In modernen Kommunikationsnetzen gewinnt die Kommunikationssicherheit zunehmend an Bedeutung. Dabei sind wichtige Aspekte der Kommunikationssicherheit die Authentizität der Teilnehmer und die Vertraulichkeit von Nachrichten. Zur Teilnahme an einer Kommunikation innerhalb von Netzwerken kann außerdem eine Autorisierung erforderlich sein. Diese Kommunikationssicherheit wird üblicherweise mit voradministrierten, gemeinsamen Geheimnissen wie beispielsweise shared secrets verwirklicht. Des weiteren kann auch mit digitalen Signaturen/Zertifikaten die Kommunikationssicherheit gewährleistet werden. Dabei erhält jeder zur sicheren Kommunikation autorisierte Netzteilnehmer ein eigenes digitales Zertifikat von einer vertrauenswürdigen zentralen Instanz. Diese Zertifikate binden einen öffentlichen Schlüssel an die Identität seines Eigentümers. Diese Zertifikate können überprüft werden mit dem öffentlichen Schlüssel der zentralen Instanz, der im sogenannten Root-Zertifikat der zentralen Instanz enthalten ist, welches unverfälscht an alle Netzwerkteilnehmer verteilt werden muss. Ein Netzteilnehmer kann nun mit seinem geheimen privaten Schlüssel eine signierte Nachricht erzeugen, deren Authentizität von jedem Empfänger mittels des öffentlichen Schlüssel aus dem Zertifikat des Netzteilnehmers geprüft werden kann. Das Zertifikat eines Netzteilnehmers erhält der Empfänger entweder von Netzteilnehmer selbst oder von einem zentralen Server. Zur vertraulichen Übermittlung von Nachrichten werden diese mit dem öffentlichen Schlüssel aus dem Zertifikat des Empfängers verschlüsselt, so dass nur dieser die Nachricht wieder entschlüsseln kann.

In einem Peer-to-Peer Netzwerk, nachfolgend mit P2P Netzwerk abgekürzt, finden Sicherheitsfunktionen wie Authentisierung, Autorisierung und Ver-/Entschlüsselung ebenso Anwendung. Wer-

den danach Informationen aus dem Zertifikat eines Netzteilnehmers benötigt, so kann das Zertifikat von dieser Netzeinheit selbst oder falls vorhanden von einer externen Speichereinheit angefordert werden.

Die bisher beschriebene Authentisierung von Daten oder Nachrichten einer Netzeinheit in einem P2P Netzwerk bringt jedoch den Nachteil mit sich, das ein Zertifikatsserver für die Teilnehmer des P2P Netzwerks zur Verfügung stehen muss und/oder die Netzteilnehmer ständig im Online-Betrieb sich befinden müssen. Darüber hinaus können auch keine vertraulichen Nachrichten für Netzteilnehmer allgemein noch für bestimmte Netzteilnehmer hinterlegt werden, wenn oben genannte Netz- und Netzteilnehmerbedingungen vorliegen.

Der Erfindung liegt die Aufgabe zugrunde, eine Schaltungsanordnung und ein dazugehöriges Verfahren zur Absicherung der Kommunikation von Netzteilnehmern anzugeben.

Die Aufgabe wird durch die Merkmale der Ansprüche 1 und 4 gelöst.

Die Erfindung bringt den Vorteil mit sich, dass eine Authentizitätsprüfung auch bei einem Offline-Betrieb des Netzteilnehmers durchgeführt werden kann.

Die Erfindung bringt den Vorteil mit sich, dass eine Autorisierungsprüfung über das Zertifikat des Netzteilnehmers auch bei einem Offline-Betrieb des Netzteilnehmers durchgeführt werden kann.

Die Erfindung bringt den Vorteil mit sich, dass eine vertrauliche Informationshinterlegung auch in einem Offline-Betrieb des Netzteilnehmers im P2P Netzwerk durchgeführt werden kann.

Die Erfindung bringt den Vorteil mit sich, dass Server zur Bereitstellung von erstellten und abgespeicherten Zertifika-

ten im laufenden Betrieb nicht erforderlich sind.

Weitere Besonderheiten der Erfindung werden aus den nachfolgenden näheren Erläuterungen zu den Figuren eines Ausführungsbeispiels ersichtlich.

Es zeigen:
Figur 1 ein P2P-Netzwerk innerhalb eines IP-Netzwerkes,
Figur 2 eine Zuteilung eines Zertifikates für einen neuen Netzteilnehmer und deren Verteilung im P2P-Netzwerk,
Figur 3 eine schematische Darstellung der Authentisierung der Nachricht eines Netzteilnehmers,
Figur 4 einen Aufbau von Schaltungsmodulen innerhalb eines Peers,
Figur 5 ein Ablaufdiagramm einer Zertifikatsverteilung,
Figur 6 ein Ablaufdiagramm einer Authentizitätsprüfung und
Figur 7 ein Ablaufdiagramm einer verschlüsselten Hinterlegung.

Anhand einer Schaltungsanordnung und dem dazugehörigen Verfahren zur Authentisierung eines Netzteilnehmers wird ein digitales Zertifikat als Ressource im P2P-Netzwerk abgespeichert. Dies bringt den Vorteil mit sich, dass Daten auch dann den weiteren Netzteilnehmern zur Verfügung gestellt werden können, wenn die oder der Netzteilnehmer im Betriebsmodus Offline oder aus anderen Gründen nicht erreichbar ist. Des weiteren ist es auch möglich, für Netzeinheiten bestimmte Daten verschlüsselt und somit geschützt im P2P-Netzwerk abzulegen.

Figur 1 zeigt ein P2P-Netzwerk innerhalb eines mit IP bezeichneten Netzwerkes.
Der Datentransfer bis zur Transportschicht findet über gebräuchliche Protokolle, beispielsweise das Internetprotokoll, statt. Zwischen dieser Transportschicht und der Anwendungsschicht befindet sich als zusätzliche Schicht die Schicht des

P2P Protokolls, welche die Zuordnung von Identifikation ID zu anderen Teilnehmern und Datensätzern vornimmt, das Abspeichern, Extrahieren sowie die Replikation von Datensätzen regelt etc.

Die mit Peer bezeichneten Elemente Peer A, Peer B,..., Peer N des P2P Netzwerkes sind beispielsweise selbständige Rechner, die untereinander beispielsweise sowohl über IP-Protokoll als auch über P2P Protokoll miteinander verbunden sind. Die hier vorausgesetzte Technologie eines P2P Netzwerkes ist beispielsweise aus einer Diplomarbeit von Thomas Friese an der Philipps-Universität Marburg zum Thema - Selbstorganisierende Peer-to-Peer Netzwerke vom März 2002 bekannt.
Innerhalb des IP-Netzes kann ebenso ein Server bzw. Zertifikatsserver beispielsweise eines Diensteanbieters angeordnet sein.

Der Gegenstand der Erfindungen wird anhand der nachfolgenden Figurenbeschreibung verdeutlicht. Ein mit Peer X bezeichnetes Netzelement soll dabei beispielsweise Zugang zu Netzteilnehmern eines mit P2P bezeichneten Netzwerkes erhalten.

In Figur 2 wird schematisch der Zugang des Netzteilnehmers Peer X zum P2P Netzwerk erläutert. In einem ersten Verfahrensschritt wird vom Netzteilnehmer Peer X, der beispielsweise ein Rechner sein kann, ein Zertifikat ZX von einem Anbieter FIRM angefordert bzw. beantragt. Der Anbieter FIRM sendet dem Antragsteller Peer X das zugeteilte und ebenfalls im Zertifikatsserver CA hinterlegte Zertifikat. Dieses vom Zertifikatserver angelegte Zertifikat ZX für den Netzteilnehmer Peer X besteht beispielsweise aus verschiedenen Rubriken wie Name des Anbieters, der Firma oder des Trustcenters der das Zertifikat vergibt, einer Seriennummer des Zertifikates, einen öffentlichen Schlüssel von Peer X, einem Gültigkeitszeitraum, einem Namen, wem der Schlüssel (Peer X) gehört und eine Signatur, die von dem Anbieter oder Trustcenter erzeugt wird. Mit der Signatur wird sichergestellt, dass die in dem Zertifikat hinterlegten Daten nur von dem Trustcenter bzw. der

Firma oder dem Anbieter vergeben wurden. Dieses Zertifikat ZX wird in einem zweiten Schritt an den neuen Netzteilnehmer Peer X des P2P-Netzwerkes gesendet. Ebenso wird vom Zertifikatsserver CA, der das P2P-Netzwerk als Ganzes betrachtet, das Zertifikat ZX auch an das P2P-Netzwerk gesendet. Beispielsweise sendet der Zertifikatsserver CA das Zertifikat ZX dazu an den Peer A. Das Peer A kann hierbei eine Gatewayfunktion übernehmen. Das Zertifikat ZX wird dann innerhalb des P2P Netzwerkes als Ressource beispielsweise im Peer M abgespeichert.

Mit der Abspeicherung des digitalen Zertifikats als Ressource im P2P-Netzwerk stehen die Informationen des digitalen Zertifikates auch dann den Netzteilnehmern des P2P Netzwerkes zur Verfügung, wenn die Netzeinheit Peer X im Betriebsmodus Offline oder aus anderen Gründen nicht erreichbar ist. Die Gültigkeitsdauer dieser Ressource entspricht dabei der Gültigkeitsdauer des Zertifikates. Somit ist es möglich, auf einen öffentlichen Schlüssel, der im Zertifikat hinterlegt ist, zuzugreifen, um die in einer Netzeinheit im P2P Netzwerk hinterlegte und signierte Informationen auf deren Authentizität hin zu überprüfen. Die Autorisierung des Zertifikatsverwenders ergibt sich aus dem Besitz eines gültigen Zertifikates, welches vom Anbieter FIRM ausgegeben wurde. Des weiteren ist es auch möglich, für einen Netzteilnehmer bestimmte Information verschlüsselt und somit geschützt im P2P-Netz abzulegen. Damit könnte beispielsweise eine vertrauliche Anruferbeantworterfunktion realisiert werden.

In Figur 3 ist schematisch wiedergegeben, wie der Netzteilnehmer Peer C eine Nachricht von Netzteilnehmer Peer X erhält, deren Authentizität von Peer C geprüft werden soll. Dazu benötigt Peer C das Zertifikat ZX von Peer X. Dieses Zertifikat ZX extrahiert Peer C aus dem P2P Netzwerk und läd es in seinen Speicher: Dazu bestimmt Peer C die Identifikation ID des Zertifikats ZX, nach der im verwendeten P2P Algorithmus festgelegten Methode, und sucht anschließend mit der im

verwendeten P2P Algorithmus festgelegten Methode nach einem Peer, dessen Identifikation mit der ID des Zertifikates möglichst gut übereinstimmt, und in dessen Speicher das Zertifikat ZX daher abgelegt wurde.

Nachdem das Zertifikat ZX in der Ressource des Netzteilnehmers Peer M gefunden wurde, wird das Zertifikat ZX an den suchenden Netzteilnehmer Peer C gesendet. Dieser überprüft nun zuerst die Gültigkeit des Zertifikates ZX mittels des öffentlichen Schlüssels QCA aus dem Rootzertifikat ZCA; anschließend prüft er die Authentizität der Nachricht mittels des öffentlichen Schlüssels QX, welcher im Zertifikat ZX enthalten ist. Ist die Authentizität bestätigt, wird die Nachricht bearbeitet; ansonsten wird sie ignoriert.

In Figur 4 ist schematisch der Aufbau eines Netzteilnehmers Peer A beschrieben. Für das Verständnis der Erfindung sind in die Darstellung ein Netzwerkmodul NWM, ein erstes Speichermodul SMPA, SMCA, SMA,.. und ein zweites Speichermodul SMX, SMY,... , ein Kryptomodul KRM sowie ein mit diesen Modulen in Verbindung stehender Prozessor P aufgenommen. Das Netzwerkmodul NWM mit Netzwerkkarte und dazugehöriger Software etc. regelt die Kommunikation mit allen externen Geräten, z.B. zwischen Peers im P2P-Netzwerk sowie auf der Internetprotokollbasierten IP-Ebene. In dem Speichermodul SMPA ist ein privater Schlüssel PA von Peer A abgespeichert; dieser muss vom Peer A geheim gehalten werden. Im Speichermodul SMA ist das Zertifikat von Peer A mit öffentlichem Schlüssel QA sowie im Speichermodul SMCA ist ein Zertifikat von Server CA mit öffentlichem Schlüssel QCA. Diese ersten 3 Datensätze sind in jedem Peer immer vorhanden. In einem zweites Speichermodul sind Zertifikate von anderen Peers X,Y,... abgelegt; diese werden bei Bedarf aus dem P2P-Netzwerk geholt. Das Kryptomodul KRW, das Software- und/oder Hardwaremäßig ausgebildet ist, verfügt dabei über Funktionen wie: Erzeugung einer digitalen Signatur mit Hilfe des privaten Schlüssels PA. Authentizitätsprüfung der digitalen Signatur von beliebigem Peer X mittels dessen öffentlichen Schlüssel QX, welcher im Zertifi-

kat von X enthalten ist. Gültigkeitsprüfung eines digitalen Zertifikates über die Authentizitätsprüfung seiner digitalen Signatur, erstellt vom Server CA mittels dessen öffentlichen Schlüssel QCA, welcher im (Root-) Zertifikat von CA enthalten ist. Verschlüsselung einer vertraulichen Nachricht an Peer X mittels des öffentlichen Schlüssels QX aus dem Zertifikat von Peer X. Entschlüsselung einer vertraulichen Nachricht von Peer X an Peer A mittels des privaten Schlüssels PA von Peer A.

In Figur 5 ist ein Programmablauf einer Zertifikatsverteilung wie in Fig.2 schematisch dargestellt wiedergegeben. Zur Zertifikatsverteilung sei in einer Vorbemerkung angegeben, dass alle Netzteilnehmer im P2P-Netzwerk ein selbstsigniertes Zertifikat des Zertifikatserzeugungsservers CA fest integriert haben. Damit hat jeder Netzteilnehmer einen öffentlichen Schlüssel QCA des Zertifikatserzeugnisservers CA. Alle Peers A, B,...N haben weiterhin eine Identifikation ID, diese Identifikation ID ist beispielsweise die Netzwerk-Adresse in dem genannten P2P-Netzwerk. Der Zertifikatserzeugungsserver CA hat das Zertifikat ZX für den Netzteilnehmer Peer X des P2P Netzwerkes erzeugt, d.h. mit seinem privaten Schlüssel PCA des Servers signiert. Dieses Zertifikat bindet einen öffentlichen Schlüssel QX an dessen Identität X.

Eine Zertifikatsverteilung erfolgt danach nach folgenden Verfahrensschritten: Der Server sendet ein Zertifikat an einen bestimmten Peer. Im vorliegenden Beispiel ist dieser der Peer A im P2P Netzwerk. Im Peer A kann die Signatur des Zertifikats ZX mittels des ihm bekannten öffentlichen Schlüssels QCA geprüft werden. Falls die Signatur als ungültig festgestellt wird, wird das Zertifikat nicht weitergeleitet, sondern gelöscht. Auch ist es möglich, dass der Zertifikats-Server selbst ein solcher Netzteilnehmer im P2P-Netzwerk ist.

In Peer A wird die Identifikation ID, die bestimmt auf welchen Peers eine Ressource im P2P Netzwerk abgelegt wird, des

Zertifikates ZX nach einer in P2P Netzwerken üblichen Methode festgelegt, die vom verwendeten P2P Algorithmus/Protokoll abhängt. Zu P2P Algorithmen/Protokollen siehe beispielsweise Petar Maymounkov, David Mazieres, New York University, Kademlia: A Peer to Peer Information System Based on XOR Metric, 2001
oder Stoica, Morris, Karger, Kaashoek, Balakrishnan, MIT Laboratory for Computer Science: Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications, August 2001.
Beispielsweise berechnet der Peer A diese ID des Zertifikates derart, dass sie aus einer eindeutigen Kennzeichnung vom Peer X hervorgeht, so dass das Zertifikat allein unter Kenntnis dieser Kennzeichnung im P2P Netz gefunden und extrahiert werden kann.

Peer A sucht sich innerhalb des P2P-Netzwerkes den Peer M, dessen Identifikation ID mit der ID des Zertifikates am besten übereinstimmt. Die Übereinstimmung bezieht sich auf eine Metrik des P2P-Netzwerksystems.

Der Peer A sendet das Zertifikat ZX an Peer M.

Im Rechner Peer M kann die Signatur des Zertifikates mittels des öffentlichen Schlüssels QCA auch überprüft werden. Ist diese o.k., speichert er das Zertifikat ab, ansonsten wird das Zertifikat gelöscht.

Das Zertifikat von Peer X ist im P2P-Netzwerk wie oben beschrieben als Ressource verfügbar, d.h. es kann von jedem Peer A,B,...N, der es benötigt, im P2P-Netzwerk gesucht und extrahiert werden. Die Erfindung bringt somit den Vorteil mit sich, dass das Zertifikat ZX auch dann noch verfügbar ist, wenn der Server und Peer X nicht verfügbar sind.

In Figur 6 ist schematisch ein Ablaufdiagramm einer Authentizitätsprüfung wiedergegeben. Zur Authentizitätsprüfung sei

angemerkt, dass alle Peers im P2P-Netzwerk selbstsignierte Zertifikate des Zertifikatserzeugungsservers CA fest integriert haben. Damit hat jeder Peer A,B,... N, einen öffentlichen Schlüssel QCA des Zertifikatserzeugungsservers CA. Alle Peers A,B,...,N, haben eine Identifikation ID, die als Netzwerkadresse im P2P-Netzwerk dient. Das Zertifikat für Peer X liegt als Ressource im P2P-Netz. So kann beispielsweise ein Datensatz wie beispielsweise ein Datenfile, Serviceanfrage oder Nachricht..., von dem Peer X mit seinem privaten Schlüssel PX signiert und an Peer C gesendet oder im P2P-Netzwerk in einem anderen Rechner Peer M, ..., Peer N, abgelegt werden. Der Peer C erhält diesen Datensatz vom Peer X oder von einem dritten Rechner Peer M.

Peer C benötigt jetzt zur Authentizitätsprüfung, also zur Prüfung, dass der Datensatz also wirklich von Peer X, stammt, dessen Zertifikat ZX.

Peer C bestimmt z.B. aus einer eindeutigen Kennzeichnung von Peer X die Identifikation ID des Zertifikates von Peer X.

In einem nachfolgenden Verfahrenabschnitt sucht Peer C mit dieser ID einen Netzteilnehmer, auf dem das Zertifikat gespeichert ist, und erhält Peer M als Ziel.

Der Rechner Peer C veranlasst Peer M, ihm das Zertifikat zu schicken. In Peer C wird nun die Gültigkeit des Zertifikates ZX überprüft und anschließend die Authentizität des von Peer X erhaltenen Datensatzes geprüft. Falls das Zertifikat und die Authentizität o.k. sind, bearbeitet Peer C den Datensatz, der von Peer X gesendet wurde. Damit ist auch eine Zugangskontrolle des P2P Netzes möglich: Nur Teilnehmer , die ein Zertifikat, vom Zertifikatserzeugungsserver CA erhalten haben, sind autorisiert, Datensätze zur Bearbeitung durch andere Teilnehmer zu erzeugen.

Aufgrund der Hinterlegung des Zertifikates in den Ressourcen

des P2P-Netzes kann jeder Peer A,B,..N, nun die Authentizität von Datensätzen im Netz im P2P-Netzwerk überprüfen. Die Überprüfung kann auch dann noch abgewickelt werden, wenn der Server und der Netzteilnehmer Peer X nicht verfügbar sind.

In Figur 7 ist schematisch der Ablauf einer verschlüsselten Hinterlegung wiedergegeben. Der nachfolgende Ablauf einer verschlüsselten Hinterlegung erfolgt ähnlich der wie zuvor beschriebenen Authentizitätsprüfung. Ausgehend von Peer C soll eine verschlüsselte Nachricht an Peer X im Netzwerk hinterlegt werden. Der Rechner Peer C bestimmt z.B. aus einer eindeutigen Kennzeichnung von Peer X die ID des Zertifikates von Peer X. Der Rechner Peer C sucht mit dieser ID einen Peer auf dem das Zertifikat gespeichert ist, und erhält Peer M als Ziel. Der Rechner Peer C veranlasst Peer M, ihm das Zertifikat zu schicken. Peer C überprüft die Gültigkeit des Zertifikates von Peer X. In Peer C wird die Nachricht mit dem öffentlichen Schlüssel QX aus dem Zertifikat von Peer X verschlüsselt. Der Peer C kann nun die verschlüsselte Nachricht im P2P-Netz hinterlegen.

Wenn Peer X die verschlüsselte Nachricht erhält, kann nur Peer X mit seinem privaten Schlüssel PX die an ihn gerichtete Nachricht von Peer C entschlüsseln.

Mit diesem Ablauf einer verschlüsselten Hinterlegung kann jeder Peer A,B,..Peer N, verschlüsselte Nachrichten an andere Teilnehmer des P2P-Netzwerkes senden bzw. hinterlegen. Dieses Senden bzw. Hinterlegen von Nachrichten an andere Teilnehmer des P2P-Netzwerkes kann unabhängig von einem Server oder der Erreichbarkeit des Ziel-Peers erfolgen.

Verfahren zur sicheren Kommunikation von Geräten bzw. Netzteilnehmern in P2P-Netzen. In diesen Netzen werden Zertifikationsinformationen über Geräte und Anwender benötigt, um von diesen signierte Informationen auf deren Authentizität hin zu überprüfen, sowie um vertrauliche Informationen an sie ver-

schlüsselt zu übertragen. Wer diese Zertifikationsinformationen benötigt, kann sie vom Netzteilnehmer selbst oder von externen Servern anfordern. Gemäß der Erfindung wird diese Information zusätzlich als Ressource im P2P-Netzwerk abgelegt. Dies bringt den Vorteil mit sich, dass die Informationen auch dann verfügbar sind, wenn das Gerät- der Anwender nicht erreichbar sind und kein Server zur Verfügung steht. Dies bringt ebenso den weiteren Vorteil mit sich, dass die Authentizitätsprüfung dauerhaft gewährleistet ist und außerdem Informationen auch dann vertraulich hinterlegt werden, wenn Gerät und Anwender temporär nicht erreichbar sind.

Patentansprüche

1. Schaltungsanordnung zur Kommunikationssicherheit zwischen zu einem Peer-to-Peer Netzwerk gehörenden Netzteilnehmern, mit
einem Netzwerkmodul zur Kommunikation mit den weiteren Netzteilnehmern und externen nicht zum Peer-to-Peer Netzwerk gehörenden Kommunikationseinrichtungen (Server),
einem Kryptomodul zur Abwicklung von kryptographischen Aufgaben, einem ersten Teilspeichermodule aufweisenden Speichermodul (SM1) in denen zu einem ersten Netzteilnehmer Zugehörigkeitsmerkmale (PA, ZA, ZCA) abgespeichert sind,
dadurch gekennzeichnet,
dass ein zweites Speichermodul (SM2) vorgesehen ist, wobei das zweite Speichermodul (SM2) Teilspeichermodule (SMX, SMY,...) zur Zwischenspeicherung von Zertifikaten (ZX, ZY,..) weiterer Netzteilnehmer (Peer X, Peer Y,.....) aufweist und die Zertifikate dieser weiteren Netzteilnehmer jeweils von allen anderen Netzteilnehmern (Peer N, Peer M,....) angefordert werden können.

2. Schaltungsanordnung nach Anspruch 1
dadurch gekennzeichnet,
dass die externe Kommunikationseinrichtung derart ausgeprägt ist, dass digitale Zertifikate hergestellt und im zweiten Speichermodul (SM2) abgelegt werden können.

3. Schaltungsanordnung nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass diese im ersten Netzteilnehmer angeordnet ist.

4. Verfahren zur Kommunikationssicherheit zwischen zu einem Peer-to-Peer Netzwerk gehörenden Netzteilnehmern, mit
einem Netzwerkmodul zur Kommunikation mit den weiteren Netzteilnehmern und externen nicht zum Peer-to-Peer Netzwerk ge-

hörenden Kommunikationseinrichtungen (Server),
einem Kryptomodul zur Abwicklung von kryptographischen Aufgaben, einem ersten Teilspeichermodule aufweisenden Speichermodul (SM1) in denen zu einem ersten Netzteilnehmer Zugehörigkeitsmerkmale abgespeichert werden,
dadurch gekennzeichnet,
dass ein zweites Speichermodul (SM2) in Teilspeichermodule (SMX, SMY,...) zur Zwischenspeicherung von Zertifikaten (ZX, ZY,..) weiterer Netzteilnehmer (Peer X, Peer Y,.....) aufgeteilt wird und die Zertifikate dieser weiteren Netzteilnehmer von allen anderen Netzteilnehmern (Peer N, Peer M,....) angefordert werden können.

5. Verfahren nach Anspruch 4,
dadurch gekennzeichnet,
dass digitale Zertifikate in der externen Kommunikationseinrichtung erstellt werden und im zweiten Speichermodul (SM2) abgelegt werden können.

Zusammenfassung

Schaltungsanordnung und Verfahren zur Kommunikationssicherheit innerhalb von Kommunikationsnetzen

Bei dieser Schaltungsanordnung und dem dazugehörigen Verfahren zur Authentisierung eines Netzteilnehmers wird ein digitales Zertifikat als Ressource im P2P-Netzwerk abgespeichert. Dies bringt den Vorteil mit sich, dass Daten auch dann den weiteren Netzteilnehmern zur Verfügung gestellt werden können, wenn die oder der Netzteilnehmer im Betriebsmodus Offline oder aus anderen Gründen nicht erreichbar ist. Des weiteren ist es auch möglich, für Netzeinheiten bestimmte Daten verschlüsselt und somit geschützt im P2P-Netzwerk abzulegen.

Fig. 3

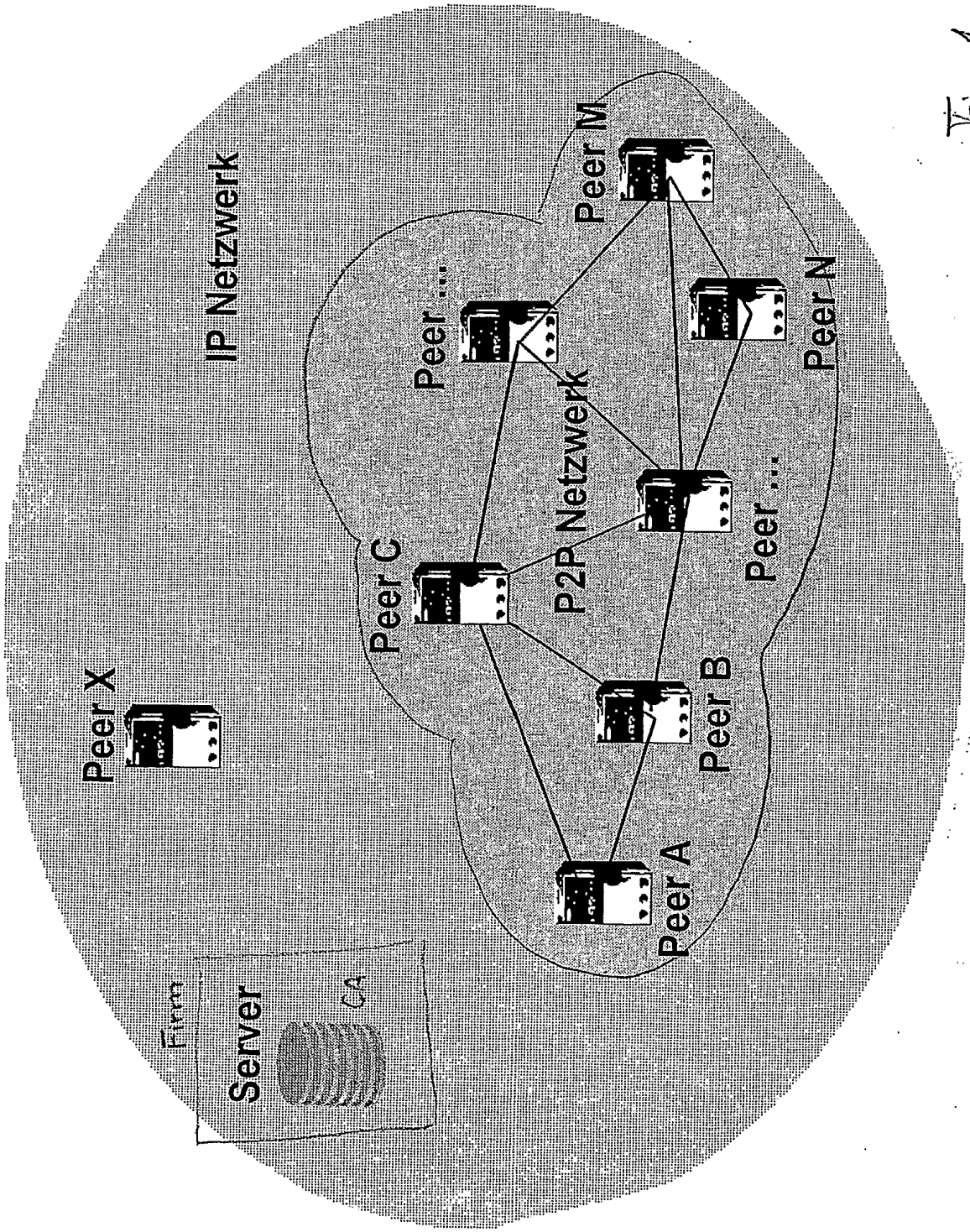
IP Netzwerk
Peer M
Peer ...
Peer N
P2P Netzwerk
Peer C
Peer ...
Peer X
Peer B
Peer A
Firma
Server
CA

Fig. 1

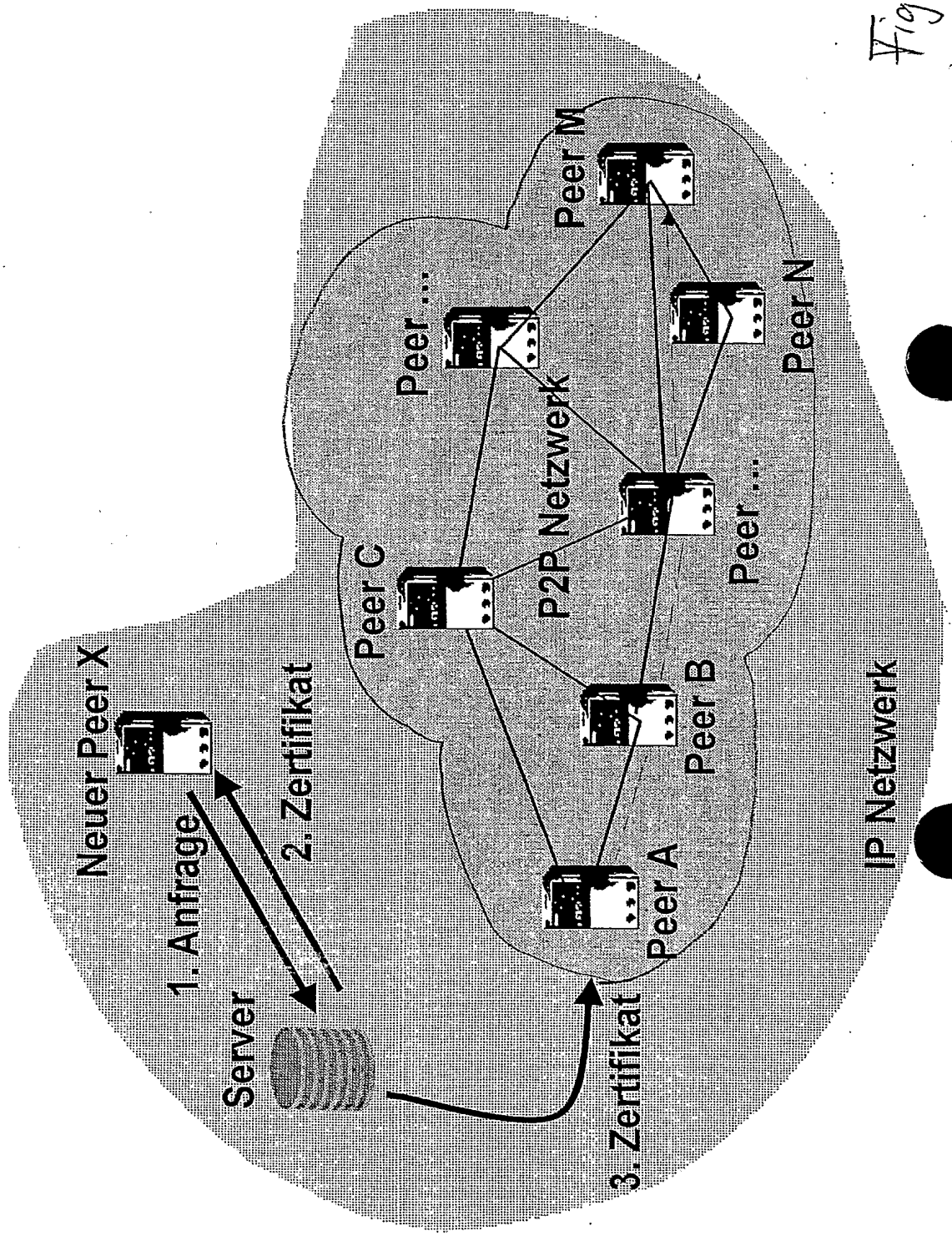
Neuer Peer X
1. Anfrage
2. Zertifikat
Server
3. Zertifikat
Peer A
Peer B
Peer C
Peer ...
Peer ...
Peer M
Peer N
P2P Netzwerk
IP Netzwerk

Fig. 2

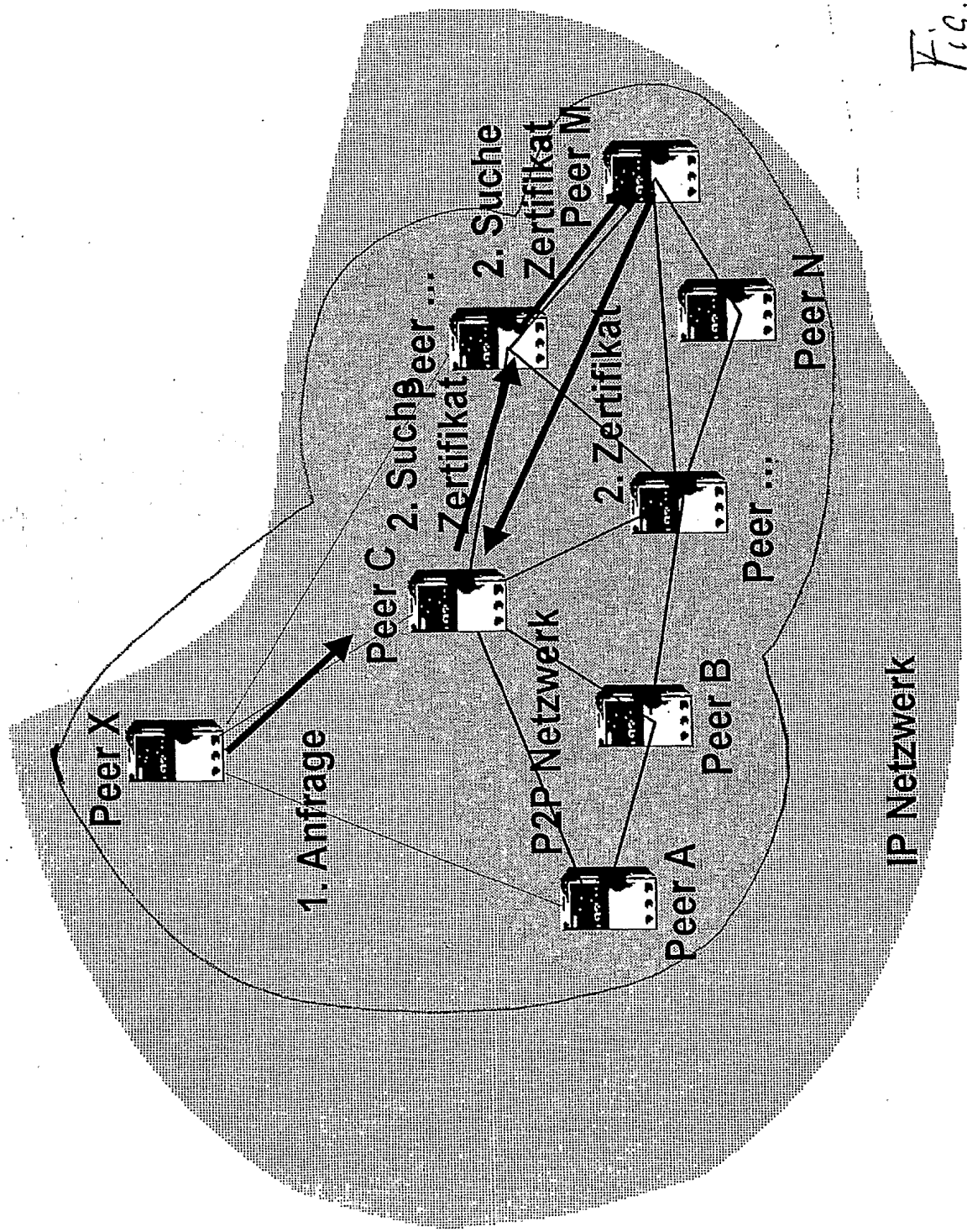
IP Netzwerk
P2P Netzwerk
Peer X
1. Anfrage
Peer C
2. Suche
Zertifikat
Peer ...
2. Suche
Zertifikat
Peer M
2. Zertifikat
Peer ...
Peer N
Peer B
Peer A

Fig. 3

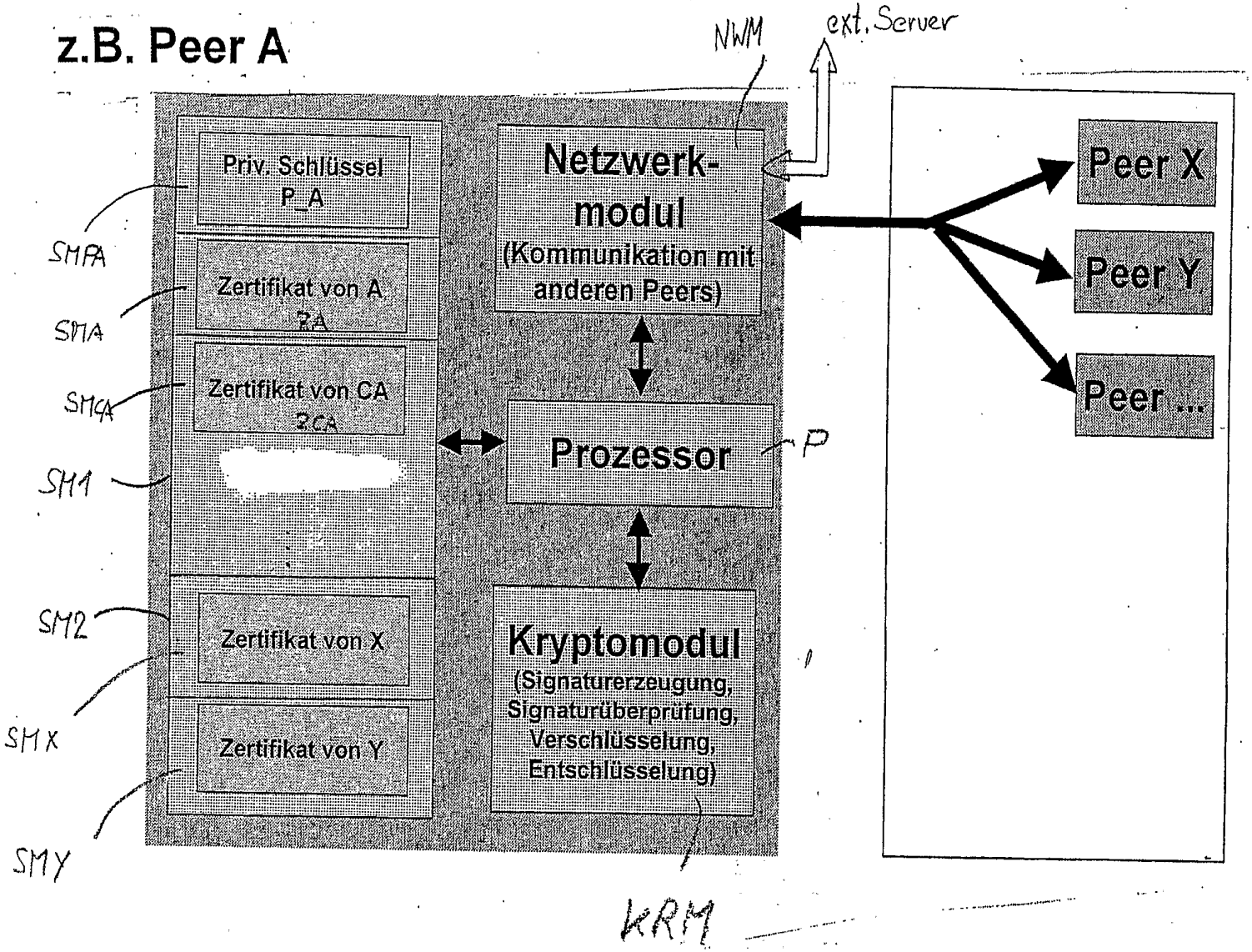
z.B. Peer A
NWM
ext. Server
Priv. Schlüssel P_A
SMPA
Zertifikat von A
SMA
Zertifikat von CA
SMCA
SM1
SM2
Zertifikat von X
SMX
Zertifikat von Y
SMY
Netzwerk-modul
(Kommunikation mit anderen Peers)
Prozessor
P
Kryptomodul
(Signaturerzeugung, Signaturüberprüfung, Verschlüsselung, Entschlüsselung)
KRM
Peer X
Peer Y
Peer ...

Fig. 4

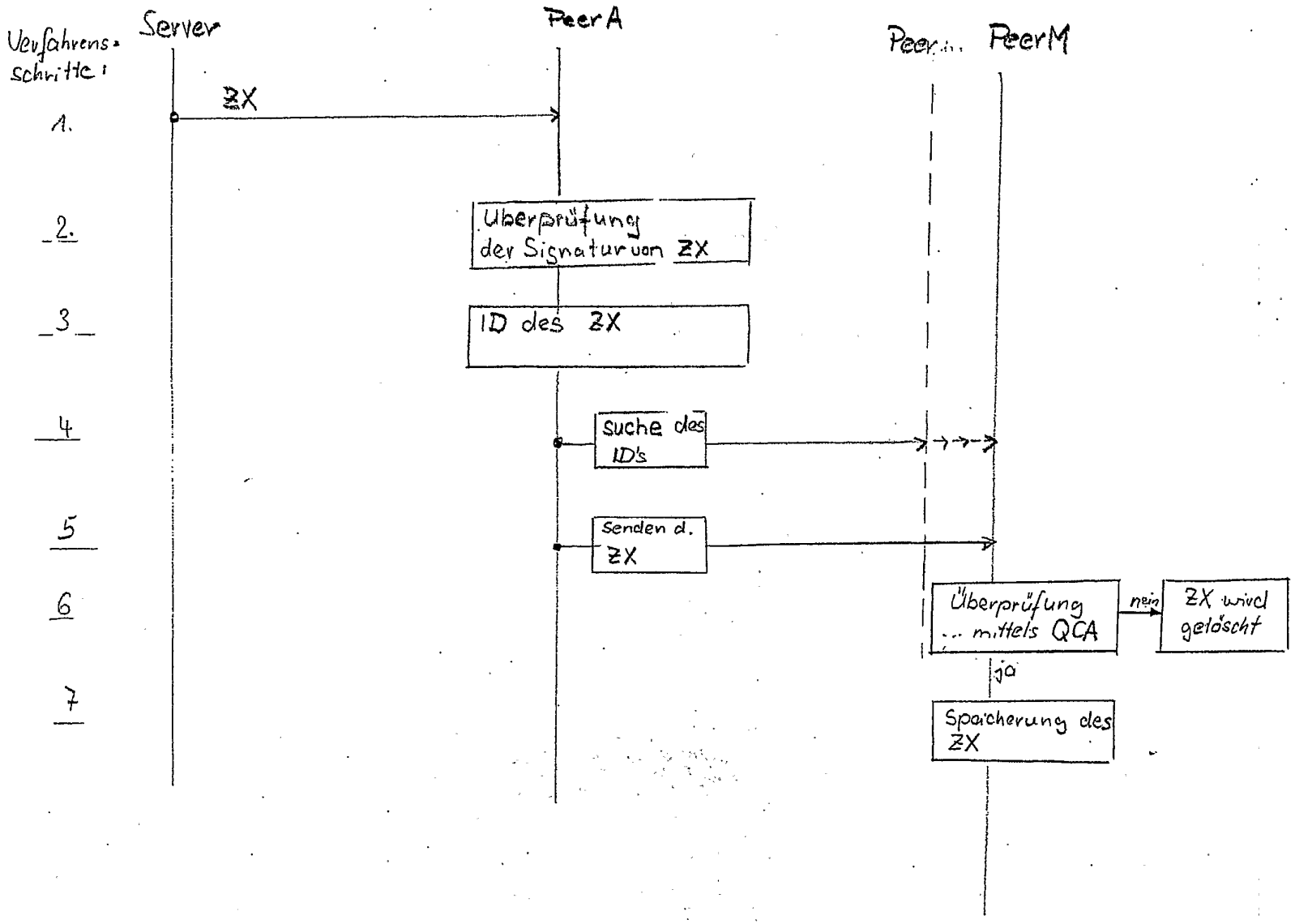
Verfahrens-schritte:
Server
Peer A
Peer...
Peer M
ZX
1.
2.
Überprüfung der Signatur von ZX
3
ID des ZX
4
Suche des ID's
5
Senden d. ZX
6
Überprüfung ... mittels QCA
nein
ZX wird gelöscht
ja
7
Speicherung des ZX

Fig. 5

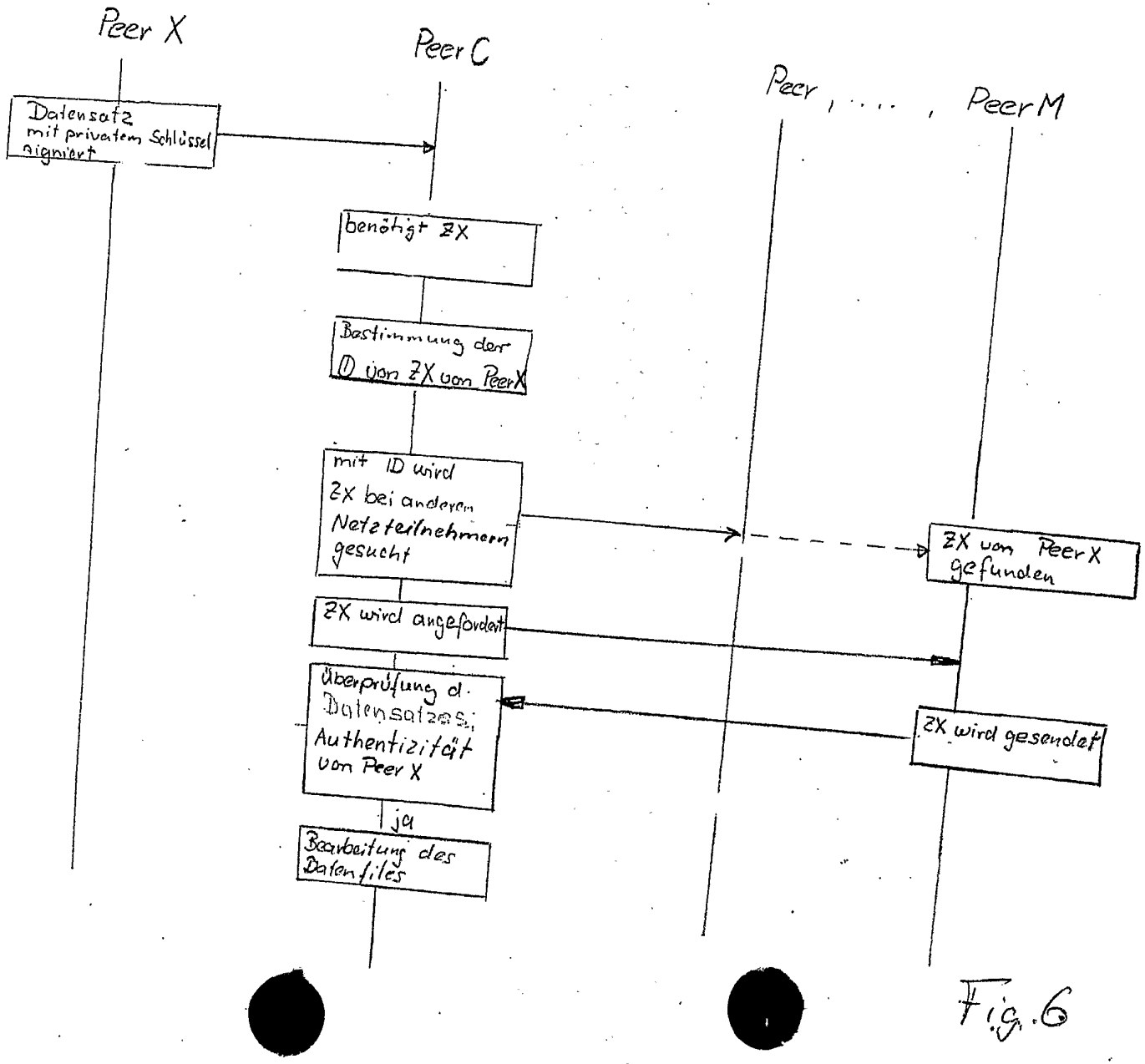
Peer X
Peer C
Peer , ... , Peer M
1.
Datensatz mit privatem Schlüssel signiert
2.
benötigt ZX
3.
Bestimmung der ID von ZX von Peer X
4.
mit ID wird ZX bei anderem Netzteilnehmern gesucht
ZX von Peer X gefunden
5
ZX wird angefordert
6
Überprüfung d. Datensatzes; Authentizität von Peer X
ZX wird gesendet
7.
ja
Bearbeitung des Datenfiles

Fig. 6

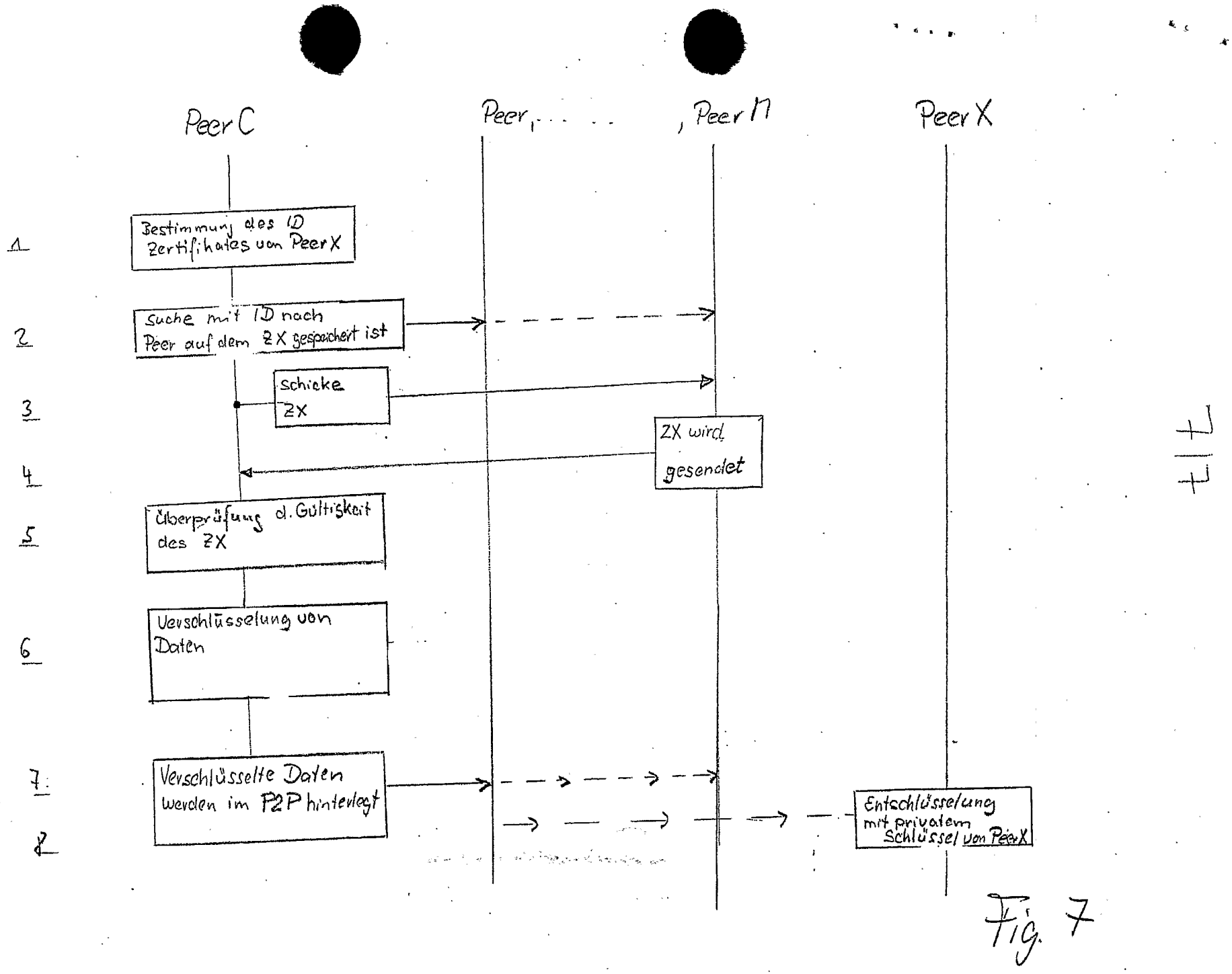
Peer C
Peer1 . . . . , Peer M
Peer X
1
Bestimmung des ID Zertifikates von Peer X
2
Suche mit ID nach Peer auf dem ZX gespeichert ist
3
schicke ZX
ZX wird gesendet
4
5
Überprüfung d. Gültigkeit des ZX
6
Verschlüsselung von Daten
7
Verschlüsselte Daten werden im P2P hinterlegt
8
Entschlüsselung mit privatem Schlüssel von Peer X

Fig. 7